



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,353	07/07/2003	Timothy J. Brown	SAFL/25C1	7913
26875	7590	08/02/2004	EXAMINER	
WOOD, HERRON & EVANS, LLP 2700 CAREW TOWER 441 VINE STREET CINCINNATI, OH 45202			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 08/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/614,353

Applicant(s)

BROWN ET AL.

Examiner

Aravind K Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 July 2003 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7/7/03
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-24 are pending in the application.
2. Claims 1-23 have been rejected.
3. Claim 24 has been objected to.

Specification

4. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Objections

5. **Claims 3, 11 and 19 objected to because of the following informalities: grammatical errors.**

As to claim 3, the "t" of the word "the" in line 1 of the claim needs to be capitalized. As to claims 11 and 19, the last word in the claim "exists" needs to be in singular form. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. **Claims 9, 10, 13-20, 23 and 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter that was not described in the specification in such a way as to reasonably convey to**

one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

After a review of the specification, there is no support for having a card reader that obtains user identification from an ID card containing the same. There is no support for the first user identification identifying the user and the second user identification identifying a group to which the user belongs.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-14 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-10 of Brown et al U.S. Patent No. 6,618,806 B1 in view of Bilich et al U.S. Patent No. 5,877,483.

As to claims 1, 9 and 10, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user

Art Unit: 2131

exists; (d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist; (e) capturing the biometric information; (f) retrieving a stored biometric information associated with the user identification; (g) comparing the captured biometric information with the retrieved biometric information; and (h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information [column 10, lines 46-67].

Brown et al does not teach that the user identification is from a card reader that obtains the user identification from an ID card containing the same. Brown et al does not teach determining an authentication rule associated with the user based on the user identification received from the card reader. Brown et al does not teach that the ID card is interacted with the card reader by swiping the ID card through the card reader.

Bilich et al teaches obtaining user identification from a card reader that obtains the user identification from an ID card containing the same. Bilich et al teaches that the ID card is interacted with the card reader by swiping the ID card through the card reader [column 3, lines 32-56].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that the user identification would have been from a card reader that obtained the user identification from an ID card containing the same. An authentication rule associated with the user would have been based on the user identification received from the card reader. The ID card would have interacted with the card reader by swiping the ID card through the card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Bilich et al because it enables user to perform typically numerous steps involved in powering up (or down) and logging on (or off) a PC with a single action, that is, a card swipe [column 2, lines 50-54].

As to claim 2, Brown et al teaches prior to step (b), further comprises the steps of: determining whether there exists an authentication rule associated with a remote computer from which the user is logging on; prompting the user to provide biometric information according to the authentication rule associated with the remote computer if it is determined that the authentication rule associated with the remote computer exists [column 11, lines 1-9].

As to claim 3, Brown et al teaches prior to step (b), further comprising the steps of: determining whether there exists an authentication rule associated with an object to which the user is being authenticated for access; prompting the user to provide biometric information according to the authentication rule associated with the object if it is determined that the authentication rule associated with the object exists [column 11, lines 11-19].

As to claim 4, Brown et al teaches after step (c) and prior to step (d), further comprising the steps of: determining whether there exists an authentication rule associated with a group to which the user belongs; prompting the user to provide biometric information according to the authentication rule associated with the group if it is determined that the authentication rule associated with the group exists; wherein step (d) includes prompting the user to provide biometric information according to the system default authentication rule associated if it is determined that both the authentication rule associated with the user and the authentication rule associated with the group do not exist [column 11, lines 20-33].

As to claim 5, Brown et al teaches that the method further comprises the steps of: determining whether there exists an authentication rule associated with an object to which the user is being authenticated for access; requesting the user to provide biometric information according to the authentication rule associated with the object if it is determined that the authentication rule associated with the object exists; determining whether there exists an authentication rule associated with a remote computer from which the user is logging on if the authentication rule associated with the object to which the user is being authenticated for access does not exist; requesting the user to provide biometric information according to the authentication rule associated with the remote computer if it is determined that the authentication rule associated with the remote computer exists; wherein step (b) includes determining whether there exists an authentication rule associated with the user if the authentication rule associated with the remote computer does not exist; determining whether there exists an authentication rule associated with a group to which the user belongs if it is determined that the authentication rule associated with the user does not exist; requesting the user to provide biometric information according to the authentication rule associated with the group if it is determined that the authentication rule associated with the group exists; wherein step (d) includes prompting the user to provide biometric information according to the system default authentication rule if it is determined that both the authentication rule associated with the user and the authentication rule associated with the group do not exist [column 11 line 34 to column 12 line 16].

As to claim 6, Brown et al teaches that the biometric information includes information relating to one or more of a finger, hand, face, voice and signature of the user [column 12, lines 17-19].

As to claim 7, Brown et al teaches that the rule includes a parameter that specifies which type of biometric information reading devices is allowable for authentication [column 12, lines 20-22].

As to claim 8, Brown et al teaches that the rule includes a parameter that specifies the confidence level of a match between the captured biometric information and the retrieved biometric information [column 12, lines 23-26].

As to claims 11, 13 and 14, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and (d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exists [column 12, lines 27-41].

Brown et al does not teach that the user identification is from a card reader that obtains the user identification from an ID card containing the same. Brown et al does not teach determining an authentication rule associated with the user based on the user identification received from the card reader. Brown et al does not teach that the ID card is interacted with the card reader by swiping the ID card through the card reader.

Bilich et al teaches obtaining user identification from a card reader that obtains the user identification from an ID card containing the same. Bilich et al teaches that the ID card is

Art Unit: 2131

interacted with the card reader by swiping the ID card through the card reader [column 3, lines 32-56].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that the user identification would have been from a card reader that obtained the user identification from an ID card containing the same. An authentication rule associated with the user would have been based on the user identification received from the card reader. The ID card would have interacted with the card reader by swiping the ID card through the card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Bilich et al because it enables user to perform typically numerous steps involved in powering up (or down) and logging on (or off) a PC with a single action, that is, a card swipe [column 2, lines 50-54].

As to claim 12, Brown et al teaches prior to step (b), the method further comprising the steps of: determining whether there exists an authentication rule associated with a remote computer from which the user is logging on; authenticating the user with the captured biometric information and the previously stored biometric information according to the authentication rule associated with the remote computer if it is determined that the authentication rule associated with the remote computer exists [column 12, lines 42-51].

8. Claims 15, 16 and 18 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 9 of Brown et al U.S. Patent No. 6,618,806 B1 in view of Kadowaki U.S. Patent No. 6,674,537 B2.

As to claim 21, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; (d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist; (e) capturing the biometric information; (f) retrieving a stored biometric information associated with the user identification; (g) comparing the captured biometric information with the retrieved biometric information; and (h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information automatically generating a user identification of a user [column 10, lines 46-67].

Brown et al does not teach receiving first and second user identification of a user from a card reader which obtains the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs. Brown et al does not teach determining whether there exists an authentication rule associated with the user based on the first user identification received from the card reader. Brown et al does not teach determining whether there exists an authentication rule associated with a group to which the user belongs based on the second user identification received from the card reader. Brown et al does not teach that if it determined that the authentication rule associated with the group does exist, prompting the user to provide biometric information according to a system default authentication rule.

Kadowaki teaches receiving first and second user identification of a user from a card reader which obtains the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs [column 11 line 37 to column 12 line 11].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that first and second user identification of a user would have been received from a card reader that obtained the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs. There would have been an authentication rule associated with the user based on the first user identification received from the card reader. It would have been determined whether there exists an authentication rule associated with a group to which the user belongs based on the second user identification received from the card reader. If it had been determined that the authentication rule associated with the group did exist, prompting the user to provide biometric information according to a system default authentication rule.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Kadowaki because it would allow a network to authenticate a user's personal information as well as to the group that the user belongs.

As to claims 16 and 18, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c)

Art Unit: 2131

authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and (d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exists [column 12, lines 27-41].

Brown et al does not teach receiving first and second user identification of a user from a card reader which obtains the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs. Brown et al does not teach determining whether there exists an authentication rule associated with the user based on the first user identification received from the card reader. Brown et al does not teach determining whether there exists an authentication rule associated with a group to which the user belongs based on the second user identification received from the card reader. Brown et al does not teach that if it determined that the authentication rule associated with the group does exit, prompting the user to provide biometric information according to a system default authentication rule.

Kadowaki teaches receiving first and second user identification of a user from a card reader which obtains the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs [column 11 line 37 to column 12 line 11].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that first and second user

Art Unit: 2131

identification of a user would have been received from a card reader that obtained the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs. There would have been an authentication rule associated with the user based on the first user identification received from the card reader. It would have been determined whether there exists an authentication rule associated with a group to which the user belongs based on the second user identification received from the card reader. If it had been determined that the authentication rule associated with the group did exist, prompting the user to provide biometric information according to a system default authentication rule.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Kadowaki because it would allow a network to authenticate a user's personal information as well as to the group that the user belongs.

9. Claims 17, 19, 20 and 23 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 9 of Brown et al U.S. Patent No. 6,618,806 B1 in view of Houvener et al U.S. Patent No. 6,070,141.

As to claims 17 and 23, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; (d) prompting the user to provide biometric information according to a system default

authentication rule if it is determined that the authentication rule associated with the user does not exist; (e) capturing the biometric information; (f) retrieving a stored biometric information associated with the user identification; (g) comparing the captured biometric information with the retrieved biometric information; and (h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information [column 10, lines 46-67].

Brown et al does not teach receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing same. Brown et al does not teach determining whether there exists an authentication rule associated with the user based on the user identification received from the keyboard or the card reader.

Houvener et al teaches receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing same [column 10, lines 34-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that the user identification would have been received from a keyboard into which the PIN was typed, and (ii) a card reader which obtains the PIN from a smart card containing the same. An authentication rule associated with the user would have been based on the PIN received from keypad.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Houvener et al because it

Art Unit: 2131

provides the extra security that the holder of the card knows the PIN number stored on the smart card. Therefore, an unauthorized user is unable to log onto the network.

As to claims 19 and 20, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and (d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist [column 12, lines 27-41].

Brown et al does not teach receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing the same. Brown et al does not teach determining whether there exists an authentication rule associated with the user based on the user identification received from the keyboard or the card reader.

Houvener et al teaches receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing same [column 10, lines 34-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that the user identification would have been received from a keyboard into which the PIN was typed, and (ii) a card reader which

Art Unit: 2131

obtains the PIN from a smart card containing the same. An authentication rule associated with the user would have been based on the PIN received from keypad.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Houvener et al because it provides the extra security that the holder of the card knows the PIN number stored on the smart card. Therefore, an unauthorized user is unable to log onto the network.

10. Claims 21 and 22 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 9 of Brown et al U.S. Patent No. 6,618,806 B1 in view of Godwin et al U.S. Patent No. 6,058,426.

As to claim 21, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; (d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist; (e) capturing the biometric information; (f) retrieving a stored biometric information associated with the user identification; (g) comparing the captured biometric information with the retrieved biometric information; and (h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information automatically generating a user identification of a user [column 10, lines 46-67].

Brown et al does not teach automatically generating a user identification of a user.

Godwin et al teaches automatically generating a user identification of a user [column 4 line 61 to column 5 line 4].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that the user identification of a user would have been automatically generated. It would have been determined whether there exists an authentication rule associated with the user based on the user identification that was automatically generated.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Godwin et al because user authorizations are easily revalidated or canceled at the same time and a high level of security is maintained at all times [column 2, lines 47-55].

As to claim 22, Brown et al discloses a method of controlling access in a computer network environment comprising the steps of: (a) receiving a user identification of a user; (b) determining whether there exists an authentication rule associated with the user; (c) authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and (d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist [column 12, lines 27-41].

Brown et al does not teach automatically generating a user identification of a user.

Godwin et al teaches automatically generating a user identification of a user [column 4 line 61 to column 5 line 4].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al so that the user identification of a user would have been automatically generated. It would have been determined whether there exists an authentication rule associated with the user based on the user identification that was automatically generated.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown et al by the teaching of Godwin et al because user authorizations are easily revalidated or canceled at the same time and a high level of security is maintained at all times [column 2, lines 47-55].

Allowable Subject Matter

11. Claim 24 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As to claim 24, Prior art does not disclose or fairly suggest (i) typing in the user identification through the keyboard and (ii) interacting an ID card containing the user identification with the card reader whereby the card reader obtains the user identification.

Art Unit: 2131


Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
July 21, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100